David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Attorneys for Plaintiff
(Additional Counsel on Signature Line)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

SARA SANGUINETTI, et al., individually and on behalf of all others similarly situated, Plaintiffs, v. NEVADA RESTAURANT SERVICES, INC., Defendant.	Case No.: 2:21-cv-01768-RFB-DJA **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**
RAYMOND D. SPEIGHT and DAVID DIETZEL, individually and on behalf of all others similarly situated, Plaintiffs, v. NEVADA RESTAURANT SERVICES, INC., Defendant.	Case No.: 2:21-cv-01780-RFB-EJY

Plaintiffs David Dietzel, Raymond D. Speight, Sara Sanguinetti, Patricia Saavedra, and Nina S. Kuhlmann ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action

against Defendant Nevada Restaurant Services, Inc. ("NRS" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack at NRS in or around January of 2021 (the "Data Breach"). The Data Breach reportedly involved at least 200,000 consumers, and perhaps as many as 300,000.

2. Information stolen in the Data Breach included individuals' sensitive information, including name, date of birth, Social Security number, driver's license number or state ID number, passport number, financial account and/or routing number, health insurance information, treatment information, biometric data, medical record, taxpayer identification number, and credit card number and/or expiration date (collectively the "Private Information" or "PII").

3. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members

that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type.

7. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

9. Because of the Data Breach, Plaintiffs and Class Members suffered injury and damages in the form of theft and misuse of their Private Information.

10. In addition, Plaintiffs' and Class Members' identities are now at risk because of Defendant' negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a further result of the Data Breach, Plaintiffs and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members have and may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiffs and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to and misuse of their Private Information from Defendant. And, Plaintiffs and Class Members presently and will continue to suffer from damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Data Breach.

16. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendant.

17. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct.

PARTIES

18. Plaintiff David Dietzel is a resident and citizen of Nevada. Plaintiff Dietzel is acting on his own behalf and on behalf of others similarly situated. NRS obtained and continues to maintain Plaintiff Dietzel Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Dietzel would not have entrusted his Private Information to NRS had he known that NRS would fail to maintain adequate data security. Plaintiff Dietzel's Private Information was compromised and disclosed as a result of the Data Breach.

19. Plaintiff Raymond Donald Speight is a resident and citizen of Nevada. Plaintiff Speight is acting on his own behalf and on behalf of others similarly situated. NRS obtained and continues to maintain Plaintiff Speight's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Speight would not have entrusted his Private Information to NRS had he known that NRS would fail to maintain adequate data security. Plaintiff Speight's Private Information was compromised and disclosed as a result of the Data Breach.

20. Plaintiff Sara Sanguinetti is a resident and citizen of Nevada. Plaintiff Sanguinetti is acting on her own behalf and on behalf of others similarly situated. NRS obtained and continues to maintain Plaintiff Sanguinetti's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Sanguinetti would not have entrusted her Private Information to NRS had she known that NRS would fail to maintain adequate data security. Plaintiff Sanguinetti's Private Information was compromised and disclosed as a result of the Data Breach.

21. Plaintiff Patricia Saavedra is a resident and citizen of California. Plaintiff Saavedra is acting on her own behalf and on behalf of others similarly situated. NRS obtained and continues to

maintain Plaintiff Saavedra's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Saavedra would not have entrusted her Private Information to NRS had she known that NRS would fail to maintain adequate data security. Plaintiff Saavedra's Private Information was compromised and disclosed as a result of the Data Breach.

22. Plaintiff Nina S. Kuhlmann is a resident and citizen of California. Plaintiff Kuhlmann is acting on her own behalf and on behalf of others similarly situated. NRS obtained and continues to maintain Plaintiff Kuhlmann's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Kuhlmann would not have entrusted her Private Information to NRS had she known that NRS would fail to maintain adequate data security. Plaintiff Kuhlmann's Private Information was compromised and disclosed as a result of the Data Breach.

23. Defendant NRS is a Nevada corporation with its principal place of business at 801 S. Rancho Dr., Ste. D-4, Las Vegas, NV, 89106.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and, upon information and belief, members of the proposed Class are citizens of states different from Defendant.

25. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Plaintiff Speight resides in this judicial district.

FACTUAL ALLEGATIONS

Defendant' Business

27. Defendant owns and operates a chain of slot machine parlors referred to as "Dotty's" with about 175 locations in Nevada, Oregon and Montana.

28. Defendant's locations offer food and beverage choices with a heavy focus on gambling.

29. In the ordinary course of doing business with Defendant, customers are required to provide Defendant with sensitive, personal and private information such as:

- Names
- Dates of birth
- Social Security numbers
- Driver's license numbers
- State ID numbers
- Passport numbers
- Financial account and/or routing numbers
- Health insurance information
- Treatment information
- Biometric data
- Medical record
- Taxpayer identification number
- Credit card numbers and/or expiration dates

30. As a condition of transacting with Defendant, Plaintiffs were required to disclose some or all of the Private Information listed above.

31. On information and belief, in the course of collecting Private Information from consumers, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures.

The Cyber-Attack and Data Breach

32. In January 2021, NRS identified the presence of malware on certain computer systems in its environment.

33. Beginning on January 16, 2021, and possibly earlier, known cybercriminals gained unauthorized access to Defendant's computer systems and networks and acquired copies of Private Information held on Defendant's systems.

34. Defendant only became aware of the unauthorized access when the cyberthieves infected Defendant's IT systems with malicious software (aka malware).

35. Forensic investigation later confirmed that the data that the cyberthieves claimed to have stolen had in fact been taken ('exfiltrated') from Defendant's computer systems.[1]

36. The cyber-attack was expressly designed and targeted to gain access to private and confidential data, including (among other things) the personal information, or PII, of Defendant's customers and clients, including Plaintiffs and Class Members. Evidence of this specific targeting of Private Information is the fact that, according to Defendant's own forensic investigation, an "unauthorized actor was able to copy" the Private Information.

37. Despite learning of the Data Breach in January 2021, Defendant failed to notify customers of the incident until eight months later, on September 3, 2021.

[1] https://sway.office.com/xD9FO63chcJBt2k1 (last accessed Sept. 22, 2021).

38. As a result of Defendant's unreasonable delay in providing notice, the risk of harm to Plaintiffs and Class Members has increased. Consumer Reports has noted: "One thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports…. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves."[2]

39. Defendant also failed to encrypt the PII stored on its server, evidenced by the fact that hackers were able to steal the Private Information in a readable form.

40. Defendant acknowledges its cybersecurity and data protection was inadequate because it admits that, "[f]ollowing the incident, NRS took immediate steps to secure its systems…."[3]

41. Defendant also acknowledges that Plaintiffs and Class Members face a substantial and present risk of identity theft because it is actively encouraging them to "remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors." [4]

42. Based on the Notice of Data Breach letter he received, which informed Plaintiffs that their Private Information was removed from Defendant' network and computer systems, Plaintiffs believe their Private Information was stolen from Defendant's networks (and subsequently sold) as a result of the Data Breach.

43. Further, the removal of the Private Information from Defendant's system demonstrates that this cyberattack was targeted.

[2] The Data Breach Next Door, Consumer Reports, Jan. 31, 2019, available at: https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Sept. 22, 2021).
[3] *Id*.
[4] https://sway.office.com/xD9FO63chcJBt2k1 (last accessed Sept. 22, 2021).

44. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

46. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the restaurant services industry preceding the date of the breach.

47. Data breaches, including those perpetrated against the restaurant services sector of the economy, have become widespread.

48. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[5]

49. According to Bluefin, "[t]he restaurant and hospitality industries have been hit particularly hard by data breaches, with hotel brands, restaurants and establishments targeted by hackers in 2019."[6]

50. Another report says that the "companies in the food and beverage industry are the most at risk from cybercriminals."[7]

51. According to Kroll, "data-breach notifications in the food and beverage industry shot up 1,300% in 2020."[8]

[5] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Sept. 22, 2021).
[6] https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/ (last accessed Sept. 22, 2021).
[7] https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack (last accessed Sept. 22, 2021).
[8] https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336 (last accessed Sept. 22, 2021).

52. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant' industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited

by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. These enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas.* (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

58. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendant was at all times fully aware of their obligation to protect the PII of customers. Defendant were also aware of the significant repercussions that would result from its failure to do so.

Defendant Fail to Comply with Industry Standards

60. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

61. Best cybersecurity practices that are standard in Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

62. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet

Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

63. These foregoing frameworks are existing and applicable industry standards in Defendant's industry. Defendant knew it was a target for hackers. Despite understanding the risks and consequences of inadequate data security, Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

Defendant's Breach

64. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

65. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

66. Accordingly, as outlined below, Plaintiffs and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

67. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

68. Defendant was well aware that the Private Information it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

71. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a

[9] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Sept. 22, 2021) ("GAO Report").

puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

72. For example, armed with just a name and date of birth, a data thief can use a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

73. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

74. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

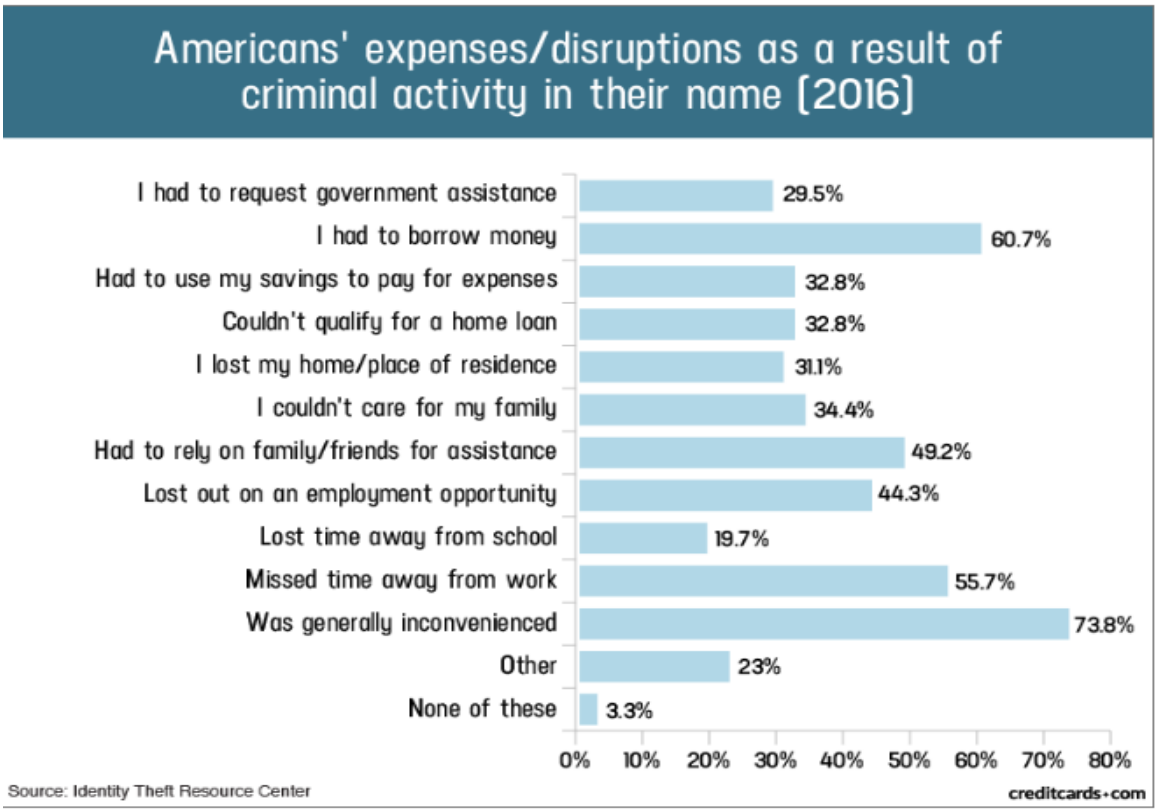
75. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

76. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

77. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[10] *See* https://www.identitytheft.gov/Steps (last accessed Sept 22, 2021).

78. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[11]



79. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[12]

80. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[11] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed September 22, 2021).

[12] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

81. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

82. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

83. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

84. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

85. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

86. Sensitive Private Information can sell for as much as $363 according to the Infosec Institute.

87. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

88. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

89. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

90. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

91. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

92. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

93. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

94. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

[13] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Sept. 22, 2021).

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[14]

96. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[15]

97. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

98. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[16] However, this is not the case. As cybersecurity experts point out:

---

[14] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Sept. 22, 2021).

[15] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed Sept. 22, 2021).

[16] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed Sept. 22, 2021).

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[17]

99. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[18]

100. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

101. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the cyber-attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the cyber-attack. The complimentary credit monitoring service offered by Defendant is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

102. Moreover, Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

103. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

---

[17] *Id.*

[18] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed Sept. 22, 2021).

Plaintiff Dietzel's Experience

104. Plaintiff Dietzel was required to provide his Private Information to Nevada Restaurant Services in connection with his being a customer of NRS beginning in or around 2005 and continuing through the present.

105. In or around July 2021, Plaintiff Dietzel received notice from NRS that his Private Information had been improperly accessed and/or obtained by unauthorized third parties that targeted and attacked NRS's "computer systems" with "malware." This notice indicated that Plaintiff Dietzel's Private Information, including his full name, driver's license number and date of birth, was compromised as a result of the Data Breach. As a customer of Defendant, Defendant required Plaintiff Dietzel to provide it with his PII, including his name, Social Security number, driver's license number, date of birth, address, email address, and credit card information. There is no indication from Defendant that the PII was encrypted or redacted in any way.

106. As a result of the Data Breach, Plaintiff Dietzel made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching the credit monitoring and identity theft protection services offered by NRS; and communicating with IRS personnel in connection with the fraud perpetrated against him as a result of the Data Breach. Plaintiff Dietzel has spent at least 10 hours dealing with the Data Breach; valuable time Plaintiff Dietzel otherwise would have spent on other activities, including but not limited to work and/or recreation.

107. As a result of the Data Breach, unauthorized third parties filed tax documents with the Internal Revenue Service ("IRS") in early 2021, claiming Plaintiff Dietzel as a dependent. As a result of this false claim, Plaintiff Dietzel has not been able to collect any stimulus payments or child tax credits from the IRS since that time. In or about April 2021, Mr. Dietzel attempted to file his 2019 and 2020 tax

returns electronically, but was denied because of the false claim. He was instructed to re-file in hard copy and include an IRS "identity theft" document, which he filed in or about May 2021. In or about mid-October 2021, the IRS instructed Mr. Dietzel to re-file those documents. In addition to not receiving stimulus and child tax credit payments, and as a result of the Data Breach and the IRS's pending investigation, Plaintiff Dietzel has still not received his expected tax returns for the 2019 and 2020 tax years.

108. As a result of the Data Breach, Plaintiff Dietzel has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Dietzel is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. Plaintiff Dietzel suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that NRS obtained from Plaintiff Dietzel; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

110. As a result of the Data Breach, Plaintiff Dietzel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Dietzel will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Speight's Experience

111. Plaintiff Speight was required to provide his Private Information to Nevada Restaurant Services in connection with his being a customer of NRS beginning in or around 2005 and continuing through in or around 2017.

112. In or around July 2021, Plaintiff Speight received notice from NRS that his Private Information had been improperly accessed and/or obtained by unauthorized third parties that targeted and attacked NRS's "computer systems" with "malware." This notice indicated that Plaintiff Speight's Private Information, including his full name, Social Security number, and driver's license number, was compromised as a result of the Data Breach. As a customer of Defendant, Defendant required Plaintiff Speight to provide it with his PII, including his name, Social Security number, driver's license number, date of birth, address, email address, and credit card information. There is no indication from Defendant that the PII was encrypted or redacted in any way.

113. As a result of the Data Breach, Plaintiff Speight made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by NRS; researching and continuing "scam alerts" on his credit reports from Experian, Transunion, and Equifax. Plaintiff Speight has spent at least six hours dealing with the Data Breach; valuable time Plaintiff Speight otherwise would have spent on other activities, including but not limited to work and/or recreation.

114. As a result of the Data Breach, multiple unauthorized third parties attempted to use Plaintiff Speight's name and Social Security number to secure credit. Each attempt, beginning after January 2021 but before July 1, 2021 and continuing through present, caused various credit bureaus to issue "scam alerts" to Plaintiff Speight.

115. As a result of the Data Breach, Plaintiff Speight has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private

Information for purposes of identity theft and fraud. Plaintiff Speight is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

116. Plaintiff Speight suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that NRS obtained from Plaintiff Speight; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

117. As a result of the Data Breach, Plaintiff Speight anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Speight will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Sanguinetti's Experience

118. Plaintiff Sanguinetti was required to provide her Private Information to Nevada Restaurant Services in connection with her being a customer of NRS beginning in or around 2011 and continuing through in or around 2021.

119. In or around July 2021, Plaintiff Sanguinetti received notice from NRS that her Private Information had been improperly accessed and/or obtained by unauthorized third parties that targeted and attacked NRS's "computer systems" with "malware." This notice indicated that Plaintiff Sanguinetti's Private Information, including her full name, date of birth, and driver's license number, was compromised as a result of the Data Breach. As a customer of Defendant, Defendant required Plaintiff Sanguinetti to provide it with her PII, including her full name, date of birth, and driver's license number. There is no indication from Defendant that the PII was encrypted or redacted in any way.

120. As a result of the Data Breach, Plaintiff Sanguinetti made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to:

researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring; researching and continuing "scam alerts" on her credit reports from Experian, Transunion, and Equifax. Plaintiff Sanguinetti has spent at least two hours dealing with the Data Breach; valuable time Plaintiff Sanguinetti otherwise would have spent on other activities, including but not limited to work and/or recreation.

121. As a result of the Data Breach, there was at least one unauthorized third party attempt to use Plaintiff Sanguinetti's name and Social Security number to secure credit. The attempt occurred between January 2021 but before July 1, 2021; and continuing through present, caused various credit bureaus to issue "scam alerts" to Plaintiff Sanguinetti.

122. As a result of the Data Breach, Plaintiff Sanguinetti has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Sanguinetti is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

123. Plaintiff Sanguinetti suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that NRS obtained from Plaintiff Sanguinetti; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

124. As a result of the Data Breach, Plaintiff Sanguinetti anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Sanguinetti will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Saavedra's Experience

125. Plaintiff Saavedra was required to provide her Private Information to Nevada Restaurant Services in connection with her being a customer of NRS beginning in or around 2018 and continuing through in or around 2021.

126. In or around July 2021, Plaintiff Saavedra received notice from NRS that her Private Information had been improperly accessed and/or obtained by unauthorized third parties that targeted and attacked NRS's "computer systems" with "malware." This notice indicated that Plaintiff Saavedra's Private Information, including her name, Social Security number, driver's license number, date of birth, address, and credit card information was compromised as a result of the Data Breach. As a customer of Defendant, Defendant required Plaintiff Saavedra to provide it with her PII, including her name, Social Security number, driver's license number, date of birth, address, and credit card information. There is no indication from Defendant that the PII was encrypted or redacted in any way.

127. As a result of the Data Breach, Plaintiff Saavedra made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Bank of America; researching and continuing "scam alerts" on her credit reports from Experian, Transunion, and Equifax. Plaintiff Saavedra has spent at least two hours dealing with the Data Breach; valuable time Plaintiff Saavedra otherwise would have spent on other activities, including but not limited to work and/or recreation.

128. As a result of the Data Breach, at least one unauthorized party attempted to misuse Plaintiff Saavedra's Private Information. Specifically, Plaintiff Saavedra was notified that an unauthorized party attempted to access her bank account.

129. Plaintiff Saavedra has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Saavedra is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

130. Plaintiff Saavedra suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that NRS obtained from Plaintiff Sanguinetti; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

131. As a result of the Data Breach, Plaintiff Saavedra anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Saavedra will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Kuhlmann's Experience

132. Plaintiff Kuhlmann was required to provide her Private Information to Nevada Restaurant Services in connection with her being a customer of NRS beginning in or around 2019 and continuing through in or around 2021.

133. In or around July 2021, Plaintiff Kuhlmann received notice from NRS that her Private Information had been improperly accessed and/or obtained by unauthorized third parties that targeted and attacked NRS's "computer systems" with "malware." This notice indicated that Plaintiff Kuhlmann's Private Information was compromised as a result of the Data Breach. As a customer of Defendant, Defendant required Plaintiff Kuhlmann to provide it with her PII, including her name, Social Security

number, driver's license number, date of birth, address, and credit card information. There is no indication from Defendant that the PII was encrypted or redacted in any way.

134. As a result of the Data Breach, Plaintiff Kuhlmann made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Kuhlmann has spent at least two hours dealing with the Data Breach; valuable time Plaintiff Kuhlmann otherwise would have spent on other activities, including but not limited to work and/or recreation.

135. As a result of the Data Breach, multiple unauthorized third parties attempted to misuse Plaintiff Kuhlmann's Private Information. For example, Plaintiff Kuhlmann received an email regarding a "NETSPEND" card that she never signed up for. The card was later delivered in the mail to Plaintiff Kuhlmann's home but she did not activate it due to the simple fact that she never applied for it. In addition, Plaintiff Kuhlmann has also received scam phone calls that appear to have been placed with the intent of committing identity theft by way of a social engineering attack.

136. As a result of the Data Breach, Plaintiff Kuhlmann has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Kuhlmann is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

137. Plaintiff Kuhlmann suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that NRS obtained from Plaintiff Kuhlmann; (b)

violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

138. As a result of the Data Breach, Plaintiff Kuhlmann anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Kuhlmann will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

139. Simply put, Plaintiffs and Class Members now face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

140. Plaintiffs and Class Members have been, and face a substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information as potential fraudsters could use that information to target such schemes more effectively.

141. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the cyber-attack.

142. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the cyber-attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

143. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant' computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

144. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

145. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the cyber-attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the cyber-attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

146. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which \remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the

storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

147. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

148. Plaintiffs and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiffs and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

149. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at a present and definitely increased risk of future harm.

CLASS ACTION ALLEGATIONS

150. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

151. Plaintiffs bring this action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23.

152. Plaintiffs propose the following Class definitions, subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seeks certification of the following Classes:

> National Class: All persons whose PII was compromised as a result of the cyber-attack that NRS discovered on or about January 16, 2021, and who were sent notice of the Data Breach.

Nevada Class: All residents of Nevada whose PII was compromised as a result of the cyber-attack that NRS discovered on or about January 16, 2021, and who were sent notice of the Data Breach.

California Class: All residents of California whose PII was compromised as a result of the cyber-attack that NRS discovered on or about January 16, 2021, and who were sent notice of the Data Breach.

Excluded from the Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

153. Plaintiffs reserve the right to amend the definitions of the Classes or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

154. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

155. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of Defendant's customers and policyholders whose data was compromised in the cyber-attack and data breach.

156. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber-attack;

c) Whether Defendant's data security systems prior to and during the cyber-attack complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the cyber-attack were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the cyber-attack;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this data breach, and whether Defendant breached that duty;

k) Whether Defendant's conduct was negligent;

l) Whether Defendant's acts, inactions, and practices complained of herein amount to an invasion of privacy;

m) Whether Defendant's actions violated federal law; and

n) Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

157. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the cyber-attack.

158. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions.

159. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

160. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

161. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

162. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 161 above as if fully set forth herein.

163. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain services, products and/or otherwise transact with Defendant.

164. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

165. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

166. Defendant's duty of care to use reasonable security measures arose Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

167. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

168. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the cyber-attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

169. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

170. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

171. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack and data breach.

172. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

173. Plaintiffs re-allege and incorporates by reference Paragraphs 1 through 161 above as if fully set forth herein.

174. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

175. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services and/or products, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

176. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant' regular business practices. Plaintiffs and Class Members accepted Defendant' offers and provided their Private Information to Defendant.

177. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

178. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

179. The protection of Plaintiffs' and Class Members' Private Information was a material aspect of the implied contracts between Defendant and its customers, including Plaintiffs and Class members.

180. On information and belief, the implied contracts – contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant' applicable privacy policy.

181. Defendant's express representations, including, but not limited to, the express representations found in its applicable privacy policy, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

182. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

183. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and paid for the services and/or products Defendant furnished in exchange for, amongst other things, the protection of their Private Information.

184. Plaintiffs and Class Members performed their obligations under the contract when they paid for their services and/or products and provided their valuable Private Information.

185. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

186. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the cyber-attack to Plaintiff and thousands of Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

187. The cyber-attack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

188. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received services and/or products that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the services and/or products with data security protection they paid for and the services and/or products they received.

189. Had Defendant disclosed that its security was inadequate or that its did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased services and/or products from Defendant.

190. As a direct and proximate result of the cyber-attack/data breach, Plaintiffs and Class Members have been harmed and have presently suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

191. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack/data breach.

192. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and All Class Members)

193. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 161 above as if fully set forth herein.

194. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

195. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

196. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

197. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

198. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

199. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

200. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

201. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT IV
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(On Behalf of Plaintiffs and the Nevada Class)

202. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

203. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states:

a. An action may be brought by any person who is a victim of consumer fraud.

b. As used in this section, "consumer fraud" means:…(e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

204. In turn, Nev. Rev. Stat. § 598.0923(2) (part of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." NRS violated this provision because it failed to disclose the material fact that its data security practices were inadequate to reasonably safeguard consumers' PII. NRS knew or should have known that its data security practices were deficient. This is true because, among other things, NRS was aware that the restaurant services industry was a frequent target of sophisticated cyberattacks. NRS knew or should have known that its data security practices were insufficient to guard against those attacks. NRS had knowledge of the facts that constituted the omission. NRS could and should have made a proper

disclosure when transacting with customers or by any other means reasonably calculated to inform consumers of its inadequate data security.

205. Also, Nev. Rev. Stat. § 598.0923(3), which is encompassed by the Nevada Consumer Fraud Act quoted above, states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." NRS violated this provision for several reasons, each of which serves as an independent act for purposes of violating § 598.0923(3).

206. *First,* NRS breached a Nevada statue requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access [or] acquisition." (Emphasis added.) NRS is a data collector as defined at Nev. Rev. Stat. § 603A.030. NRS failed to implement and maintain reasonable security measures, evidenced by the fact that hackers accessed NRS's cloud server and stole consumers' PII. NRS's violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3) because NRS knew or should have known that its data security practices were deficient. This is true because, among other things, NRS was aware that the restaurant services industry was a frequent target of sophisticated cyberattacks. NRS knew or should have known that its data security practices were insufficient to guard against those attacks. NRS had knowledge of the facts that constituted the violation.

207. *Second*, NRS breached other state statutes regarding unfair trade practices and data security requirements as alleged *infra*. Specifically, NRS violated the state statutes set forth in Counts VI-XIV. NRS also violated Nev. Rev. Stat. § 598.0923(2) as alleged above in this Count. NRS knew or should have known that it violated these statutes. NRS's violations of each of these statutes serves as a separate actionable act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

208. Third, NRS violated the FTC Act, 15 U.S.C. § 45, as alleged above. NRS knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance. This is true because, among other things, NRS was aware that the restaurant services industry was a frequent target of sophisticated cyberattacks. NRS knew or should have known that its data security practices were insufficient to guard against those attacks. NRS had knowledge of the facts that constituted the violation. NRS's violation of the FTC Act serves as a separate actionable act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

209. NRS engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Class members.

210. Plaintiffs and Class members were denied a benefit conferred on them by the Nevada legislature.

211. Nevada Rev. Stat. § 41.600(3) states that if the plaintiff prevails, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

212. As a direct and proximate result of the foregoing, Plaintiffs and Class members suffered all forms of damages alleged herein. Plaintiffs' harms constitute compensable damages for purposes of Nev. Rev. Stat. § 41.600(3).

213. Plaintiffs and Class members are also entitled to all forms of injunctive relief sought herein.

214. Plaintiffs and Class members are also entitled to an award of their attorney's fees and costs pursuant to Nev. Rev. Stat. § 41.600(3)(c).

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

215. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein, and plead this count in the alternative to the breach of contract count (Count II) above.

216. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

217. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

218. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the cyber-attack, Defendant instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize their own profits over the requisite security.

219. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

220. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

221. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

222. Plaintiffs and Class Members have no adequate remedy at law.

223. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or

unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant' possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

224. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

225. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant' services.

COUNT VI
CALIFORNIA CONSUMER PRIVACY ACT
(On Behalf of Plaintiffs Patricia Saavedra and Nina S. Kuhlmann and the California Class)

226. Plaintiffs Saavedra and Kuhlmann and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 161.

227. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiffs' and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

228. The PII of Plaintiffs and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violation of its duty under the CCPA.

229. Plaintiffs and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

230. Defendant knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as encrypting the PII so in the event of a data breach the PII cannot be read by an unauthorized third party. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiffs and members of the California Subclass was exposed.

231. Defendant is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code section 1798.140.

232. Plaintiffs and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiffs and the California Subclass. Plaintiffs and the California Subclass have an interest in ensuring that their PII is reasonably protected.

233. On November 12, 2021, Plaintiffs' counsel sent a notice letter to Defendant's registered service agents via certified mail. Assuming Defendant does not cure the effects of the Data Breach, which would require retrieving the PII or securing the PII from continuing and future use, within 30 days (Plaintiffs believe any such cure is not possible under these facts and circumstances), Plaintiffs intends to

amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

COUNT VII
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiffs Patricia Saavedra, and Nina S. Kuhlmann and the California Class)

234. Plaintiffs Saavedra and Kuhlmann and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 161.

235. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

236. Defendant stored the PII of Plaintiffs and Class Members in its computer systems.

237. Defendant knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs' and Class Members' PII secure and prevented the loss or misuse of that PII.

238. Defendant did not disclose at any time that Plaintiffs' and Class Members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

239. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of their computer systems, specifically the security thereof, and its ability to safely store Plaintiffs' and Class Members' PII.

240. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its

affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiffs and Class Members of the Data Breach.

241. If Defendant had complied with these legal requirements, Plaintiffs and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiffs and Class Members of the Data Breach.

242. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

243. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiffs' and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

244. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the harms alleged below.

245. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has

greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

246. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and Class Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, In re LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

247. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiffs and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of

pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

248. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiffs and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Classes;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant' wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: November 16, 2021 Respectfully submitted,

/s/ David Hilton Wise
David Hilton Wise, Esq.
Nevada Bar No. 11014
Joseph M. Langone, Esq.*
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro
jlangone@wiselaw.pro

M. Anderson Berry, Esq.*
Gregory Haroutunian, Esq.*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

David K. Lietz, Esq.*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dlietz@masonllp.com

Gary M. Klinger, Esq.*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

George Haines, Esq. (#9411)
Gerardo Avalos, Esq. (#15171)
FREEDOM LAW FIRM
8985 South Eastern Ave.,
Suite 350
Las Vegas, Nevada 89123

Michael Kind, Esq. (#13903)
KIND LAW
8860 South Maryland Parkway
Suite 106
Las Vegas, Nevada 89123
Attorneys for Plaintiffs and the Class

*P*ro hac vice*